# ELECTRONIC SIGNATURE GUIDELINES

**State of North Dakota**
**Information Technology Department**

**October 2004**

# ELECTRONIC SIGNATURE GUIDELINES
## TABLE OF CONTENTS

# I. INTRODUCTION

On April 3, 2001, Governor John Hoeven signed the Uniform Electronic Transactions Act (UETA) and filed it with the Secretary of State. UETA applies to electronic records and electronic signatures relating to transactions conducted after July 31, 2001. UETA and the companion federal law, Electronic Signatures in Global and National Commerce Act (ESIGN), provide assurance that electronic signatures will be granted the same legal authority as traditional ink signatures on paper. Therefore, if an electronic transaction meets the requirements of the electronic signature laws, neither party can repudiate a contract based on the fact that the transaction was conducted electronically, rather than on paper.

The Information Technology Department formed the Electronic Signatures Committee to develop guidelines for the use and acceptance of signatures in the state of North Dakota with respect to UETA and ESIGN. The Electronic Signatures Committee consists of representatives from thirteen state agencies, with legal guidance from the Attorney General's Office.

These guidelines should be used as a best practice tool and provide basic information regarding electronic signatures. Specific standards and policies related to the electronic signature technology infrastructure will be developed through the Enterprise Architecture process.

# II. BACKGROUND

The increased use of personal computers and the Internet is making electronic transactions more common every day. The North Dakota Uniform Electronic Transaction Act eliminates legal barriers to the use of electronic technology to create and sign contracts and other records, collect and store electronic records, and conduct everyday transactions electronically. Basically, the Act eliminates barriers to electronic commerce, while protecting consumers at the same level expected with paper-based transactions.

The Act is codified in Chapter 9-16 of the North Dakota Century Code. It does not apply to transactions governed by the following:

a. A law governing the creation and execution of wills, codicils, or testamentary trusts;
b. The Uniform Commercial Code other than sections 41-01-07 and 41-01-16 and chapters 41-02 and 41-02.1; and
c. Chapters 41-03, 41-04, 41-04.1, 41-05, 41-07, 41-08, or 41-09.

In addition, UETA provides an exception for records where a law was enacted after July 31, 2001 which specifically prohibits the use of an electronic signature for the specified purpose.

Along with this new found freedom to conduct electronic transactions, state agencies are still required to satisfy their records management responsibilities. When implementing electronic signatures, records coordinators and IT professionals need to be aware that signatures are an integral part of a record. The trustworthiness of the electronically-signed record needs to be maintained for the full records life cycle. The records life cycle is the life span of the record from its creation or receipt to its final disposition. It is usually described in three stages: creation, maintenance and use, and final disposition. Final

disposition can mean permanent deletion or destruction, or transfer to the State Archives if the record has historical value. Therefore, the electronic signature must remain accessible for the full retention period of the record to which it is associated.

**Definitions**

1. Agreement: the bargain of the parties in fact, as found in the parties' language or inferred from other circumstances and from rules and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.
2. Automated transaction: a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.
3. Computer program: a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.
4. Contract: the total legal obligation resulting from the parties' agreement as affected by this Act and other applicable law.
5. Electronic: relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
6. Electronic agent: a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances, in whole or in part, without review or action by an individual.
7. Electronic record: a record created, generated, sent, communicated, received, or stored by electronic means.
8. Electronic signature: an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
9. Governmental agency: an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the state.
10. Information: data, text, images, sounds, codes, computer programs, software, data bases, or the like.
11. Information processing system: an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.
12. Key Pair: a Private Key and the corresponding Public Key used in conjunction with digital signatures to validate the authenticity of an electronic document and/or signature.
13. Record: information that is inscribed on a tangible medium or which is stored in an electronic or other medium and is retrievable in perceivable form.
14. Security procedure: a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.
15. Transaction: an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

## III. THE FEDERAL ESIGN ACT AND NORTH DAKOTA

The Federal ESIGN Act (Public Law 106-229) confirms that states must allow the use of electronic signatures if the two parties involved agree to this method of signing.

ESIGN applies to interstate commerce, foreign commerce, and business transactions with the Federal Government. Impact on the State of North Dakota may be considerable, specifically for those agencies that deal with companies or organizations that are from out of state. ESIGN contains numerous consumer protection requirements. It also contains language that specifies that any requirements be technology neutral. The Tax Department, Secretary of State's Office, and Office of the Insurance Commissioner are examples of agencies that may be directly affected.

## IV. ELECTRONIC SIGNATURES

Electronic signature is a basic term for a variety of methods used as an alternative to a traditional ink signature on paper. Three basic classifications of electronic signatures exist, each with an increased level of cost, integrity, authenticity, security, and non-repudiation.

**Common Electronic Signatures**

Common electronic signatures are any signature method that does not employ a specific technology to increase the security, authenticity, or evidentiary value of a signature.

Common electronic signatures include a digitized image of a handwritten signature, a password or PIN (Personal Identification Number), "clickwrap" signature method where the user clicks a button onscreen to accept what is being stated, or a mark or symbol indicating intent to sign.

Another example of a common electronic signature is the use of the symbol "/s/". The symbol may be used in a number of ways.

- The symbol is affixed to an electronically stored document such as a letter. The symbol demonstrates that the paper copy, sent to the addressee, was signed with a traditional "wet" signature.

  Sincerely,
  /s/
  John Doe

- The symbol is used as an electronic signature on an electronically distributed document such as a memorandum or report.

  To: Project Team
  From: /s/ John Doe
  Date: 06/04/2004
  Subject: Meeting Minutes

- The symbol is used on the record copy of a document that will be distributed to a large distribution list or when the document will be posted electronically. The original document is signed with a "wet" signature and scanned for retention or archival purposes. The signature symbol is used in the distributed or posted copies.

  Signed this day,
  /s/
  Governor John Doe

**Secure Electronic Signatures**

Secure electronic signatures typically use technology to link the electronic signature to an individual or device. Secure electronic signatures may use biometric, biorhythmic, holographic, and cryptographic technology.

- Biometric signature: the automatic identification of a person based on their physical characteristics, such as a thumbprint or retina scan.

- Biorhythmic signature: the comparison of physical signature characteristics, typically speed and pressure of the stroke, to a previously provided and stored sample.

- Holographic signature: a physical likeness of an individual signature, applied electronically and bound to the content via cryptographic technology.

- Cryptography: the science of mapping readable text, called plaintext, into an unreadable format through encryption and back to readable text through decryption. This process affects the appearance of the data, without altering the content.

**Digital Signatures**

The digital signature process, in conjunction with a digital certificate, uses a private key to sign and encrypt the document and a public key to de-crypt and authenticate the signature. Digital certificates are typically issued by a trusted third party that verifies facts about your identity and issues a certificate that attests to those facts.

Digital signatures offer the highest level of authenticity, security, and integrity and are the most difficult and costly to implement.

These guidelines should be used to assist agencies in making informed decisions regarding the appropriate use of electronic signatures at each level. State agencies must determine the risks and benefits of the available technologies for their specific applications.

# V. GUIDELINES FOR TRUSTWORTHY RECORDS

A key issue with electronic signatures is proving the signature is from the person the signature represents and the document has not been altered.

**Characteristics of Trustworthy Records:**
According to the National Archives and Records Administration (NARA), the characteristics listed below are used to describe trustworthy records from a records management legal perspective.

1. Reliability: record content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or activities.

2. Authenticity: a record proven to be what it claims to be and to have been created or sent by the person who claims to have created and sent it; assurance of identity.

3. Integrity: proof that a record is complete and has not been altered.

4. Usability: a record can be located, retrieved, presented, and interpreted in connection with the business transaction that created it.

5. Signature Intent: the process used to obtain the electronic signature must demonstrate that the user intended to sign the record. Establishing intent includes:

    a. Identifying the purpose for signing the electronic record (could be apparent within the context of the transaction);
    b. Being reasonably certain the signer knows which electronic record is being signed; and
    c. Providing notice to the signer that their electronic signature is about to be applied to, or associated with, the electronic record (such as an online notice advising the signer that continuing the process will result in an electronic signature).

6. Trustworthiness of the process: The process used to conduct electronic transactions must be documented, such as in a formal procedure, and followed consistently.

7. Trustworthiness of the system
    a. Consistent: the system processes information in a manner that assures the records they create are credible.
    b. Complete: contains the content, structure, and context generated by the transaction they document.
    c. Accurate: quality controlled at input to ensure the information in the system correctly reflects what was communicated in the transaction.
    d. Preserved: continue to reflect content, structure, and context within any system by which the records are retained over time.

    State agencies shall maintain adequate documentation of the system design, implementation, use, and migration. The documentation shall include a narrative description of the system, physical and

technical characteristics, and any other technical information required to access or process the records.

8. Non-repudiation: a property that protects against an individual or entity from denying having performed a particular action related to the data. Non-repudiation services protect the reliability, authenticity, integrity, usability, confidentiality, and legitimate use of electronically-signed information.

   Essential elements of a non-repudiation model include:
   - Evidence of the origin of the message
   - Evidence of being sent
   - Evidence of receipt
   - Timestamp, as needed, by the agency of origin
   - Long-term storage of evidence
   - Designated adjudicator of prospective disputes

**Preserving Trustworthy Records:**

For a record with an electronic signature to remain trustworthy over the record life cycle, it is necessary to preserve its content, context, and sometimes its structure.

1. Content: Includes the electronic signature and any associated date or other identifiers, such as organization or title. It provides evidence of a document's reliability and authenticity.

2. Context: Includes individual identifiers that are not embedded in the content of the record but are used to create and verify the validity of an electronic signature. It provides additional evidence to support the reliability and authenticity of the record.

3. Structure: Includes the physical and logical format of the record and the relationships between data elements comprising the record. If an agency determines it is necessary to maintain the structure of the electronic signature, it must be able to recreate the signature or demonstrate the process used to create the signature.

**Steps to Ensure Electronically-signed Records are Trustworthy:**

1. Create and maintain documentation of the systems used to create the records that contain electronic signatures.

2. Ensure records that include electronic signatures are created and maintained in a secure environment that protects the records from unauthorized alteration or destruction.

3. Implement standard operating procedures for the creation, use, and management of records that contain electronic signatures and maintain written documentation of those procedures.

4. Create and maintain records according to the documented standard operating procedures.
5. Train agency staff in the standard operating procedures.

6. Dispose of records that contain the electronic signatures and the associated records according to the established retention schedule for the agency and the ND General Retention Schedule.

## VI. GUIDELINES FOR IMPLEMENTATION OF ELECTRONIC SIGNATURES

Agencies should follow these steps to assist them in the implementation and use of electronic signatures.

1. Identify agency statutes, regulations, policies, and procedures affected by UETA to ensure the use of electronic signatures is not restricted. See examples in Appendix B.

2. Make any necessary revisions regarding the use of signatures to the affected statutes, regulations, policies, and procedures.

3. Evaluate current business processes to determine if a signature is required on a document.

4. If a signature is necessary, evaluate each business process in the areas listed below to determine which type of electronic signature meets the business requirements of that document. See Appendix D.
    a. Transaction Value and Risk: Determine the potential for loss and the value associated with the loss.
    b. Relationship of the Parties to the Transaction: Determine if the transaction is employee-to-organization, customer-to-organization, organization-to-supplier, etc. Some relationships are inherently more trusted than others.
    c. Technical Infrastructure: Look for a solution that complements or fits within the existing technology infrastructure.
    d. Business Model: Determine if the electronic signature solution supports your business model.
    e. State and Federal Regulations: Determine if any regulations prohibit or restrict the use of electronic signatures for the particular application.

## VII. GUIDELINES FOR ELECTRONIC SIGNATURES

1. The level of electronic signature selected must ensure the proper level of authentication, confidentiality, integrity, security, and non-repudiation.

2. State employees must protect and not disclose or make available their digital signature private key or password to other persons.

3. The agency must revoke or send a revocation notice to the certification authority for employees no longer authorized to conduct electronic business on behalf of the agency.

4. Agencies must document the process used to electronically sign documents and coordinate this process with the State Records Management Administrator according to N.D.C.C. 9-16-17.

A requirement for effective use of digital signatures is interoperability across agencies and other government entities. Interoperability is the ability of one system to use the parts or equipment of another system. Establishing common signing process criteria will allow for electronic signature reciprocity between states. States will be able to share signed electronic documents and rely on documents from other sources.

Several groups, including the National Governors' Association and National Electronic Commerce Coordinating Council, are working on the interoperability issues. Below are some general guidelines that are expected to be further developed or accepted in the future.

**Guidelines:**

1. Each agency that uses digital signature technology must establish a digital signature implementation and use policy that
   - describes how the agency will determine which employees will have a digital signature, the scope of the employee's authority to use the digital signature and for what purposes;
   - identifies the roles and responsibilities of issuing digital signatures, letters authorizing the issuance of certificates, procedures to protect digital signatures, and procedures for suspension or revocation of digital signature certificates;

2. The State of North Dakota will only accept digital certificates issued by authorized certification authorities.

3. Certification authorities must provide the following information or meet the following requirements to be authorized to issue digital certificates in the State of North Dakota:
   - Certification Practice Statement (CPS) that documents the practices, procedures, and controls employed by the certification authority.
   - Statement of compliance with X.509V3 Certificate.
   - Approved (registered) vendor with the North Dakota State Procurement Office.

## VIII. RECORDS RETENTION ISSUES

Records created as a result of electronic transactions must be retained according to the agency's retention schedule, the ND General Retention Schedule, and the North Dakota Electronic Records Management Guidelines.

**Guideline:**

1. Electronically signed records must contain all the information necessary to reproduce the entire electronic record and associated signatures in a form that permits the person viewing or printing the entire electronic record to verify:
   a. The contents of the electronic record;
   b. The method used to sign the electronic record, if applicable;
   c. The person(s) signing the electronic record; and
   d. The date when the signature was executed.

## IX. CONCLUSION

These guidelines are provided to assist agencies in making informed decisions regarding the appropriate use of electronic signatures at each level.

The Information Technology Department appreciates the time and assistance of all members of the Electronic Signatures Committee.

# APPENDIX A

# CONTACT INFORMATION

Dawn Cote
ITD – Records Management
600 E Boulevard Ave.
Bismarck, ND 58505-0100
701-328-3592
dcote@state.nd.us

Sharon Freeman
ITD – Records Management
600 E Boulevard Ave.
Bismarck, ND 58505-0100
701-328-3579
sfreeman@state.nd.us

Becky Lingle
ITD – Records Management
600 E Boulevard Ave.
Bismarck, ND 58505-0100
701-328-3585
blingle@state.nd.us

Bill Roach, CRM
ITD – Records Management
600 E Boulevard Ave.
Bismarck, ND 58505-0100
701-328-3589
bjroach@state.nd.us

# APPENDIX B

## EXAMPLES OF STATUTES REQUIRING A SIGNATURE OR INK

**CHAPTER 1-01-37**
**GENERAL PRINCIPLES AND DEFINITIONS**
**1-01-37. Written and printed - Definition.** The words "writing" and "written" include "typewriting" and "typewritten", and "printing" and "printed", except in the case of signatures and when the words are used by way of contrast to typewriting and printing. Writing may be made in any manner, except that when a person entitled to require the execution of writing demands that it be made with ink, it must be so made.

**CHAPTER 40-50.1**
**PLATTING OF TOWNSITES**
**40-50.1-03. Instruments of dedication - Certifying and recording plat.** The plat must contain a written instrument of dedication, which is signed and acknowledged by the owner of the land. When there is divided ownership, there must be indicated under each signature the lot or parts of lots in which each party claims an interest. All signatures on the plat must be written with black ink, not ball point. The instrument of dedication must contain a full and accurate description of the land platted. The registered land surveyor shall certify on the plat that the plat is a correct representation of the survey, that all distances are correct and monuments are placed in the ground as shown, and that the outside boundary lines are correctly designated on the plat. The dedication and certificate must be sworn to before an officer authorized to administer an oath. The plat must be presented for approval to the governing body affected by the plat, if right-of-way dedication is required, together with an attorney's opinion of title stating the name of the owner of record.

# APPENDIX C

## EXAMPLES OF LEVELS OF ELECTRONIC SIGNATURES

Level 1: Common Electronic Signature
Clicking the "Accept" button on a software agreement or typing your name at the end of an email message.

Level 2: Secure Electronic Signature
Signing a pressure-sensitive screen that compares the speed and pressure of the stroke to a previously stored sample of your signature.

Level 3: Digital Signature
Using a Public Key Insfrastructure (PKI) solution, like VeriSign, and a public key to sign and encrypt a contract and send it to another entity that has a private key to decryrpt the document.

## APPENDIX D

## DETERMINING LEVEL OF RISK AND APPROPRIATE ELECTRONIC SIGNATURE LEVEL

| Level of Risk | Relationship Between Parties | Transaction Value | Future Need to Access |
|---|---|---|---|
| Low | Intra-Agency | No funds are transferred. No legal or financial liability is involved. No confidentiality or privacy issues are involved. | Information generated will not need to be accessed again. |
| Low to Moderate | Inter-Agency | Transaction fulfills a legal duty enforced by civil or criminal liability. | Information generated may be subject to an audit. |
| Moderate | With an agency in another level of government, i.e. local, Federal, or another state | Involves confidential information. | Information generated may be subject to a dispute by one of the parties to the transaction. |
| Moderate to High | With a private organization or individual with whom the agency has an established relationship | Involves contracts or other commitments involving legal or financial liability. | Information generated may later be subject to a dispute by a non-party to the transaction. |
| High | One-time transaction with a private organization or individual | Involves the transfer of funds. | Information generated may later be needed as proof in court. |